Release Notes for the Catalyst 1900 and Catalyst 2820 Series Switches, Version 9.00.06

July, 2002

These release notes provide information on the Catalyst 1900 and Catalyst 2820 series Ethernet switches (hereafter referred to as the Catalyst 1900 switches and the Catalyst 2820 switches) using standard and Enterprise Edition firmware version 9.00.06.

Note This document describes the problems that are resolved in versions 9.00.00 through 9.00.06.

Contents

This document has these sections:

The tracking numbers for some items in this document are added for your convenience.

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Using Previous Releases of the Switch Firmware

The Catalyst 1900 and Catalyst 2820 switches are shipped with firmware version 9.00.05. Depending on the board version of your switch, you need the minimum firmware releases listed in Table 1.

The "System Revision" field on the System Configuration menu displays the board revision of your switch. When you use the **show version** command from the command-line interface (CLI), the "Hardware Board Revision Is" field displays the board revision.

The Firmware Configuration Menu and the Console and Upgrade Configuration page display the firmware version in use.

Table 1 Supported Firmware on the Catalyst 1900 and Catalyst 2820 Switches

Board Revision	Switch	Supported Firmware Version
1	Catalyst 1900-A Catalyst 1900-EN	6.x or later
1	Catalyst 2820-A Catalyst 2820-EN	6.x or later
4	Catalyst 1900-A Catalyst 1900-EN	8.00.04 or later
5	Catalyst 1900-A Catalyst 1900-EN	8.01.00 or later
5	Catalyst 2820-A Catalyst 2820-EN	8.01.01 or later

Supported Browsers

To use the Catalyst 1900 or Catalyst 2820 Switch Manager, you must have one of these web browsers installed on your management station:

Table 2 Browser Support for Web-Based Management

Browser	Minimum Version	Supported Version
Netscape Communicator	4.5	4.5, 4.51, 4.61
Microsoft Internet Explorer	4.01a	4.01a, 5.0

Note Netscape Communicator 4.60 is not a supported browser. Microsoft Internet Explorer is not a supported browser on Solaris 2.5.1 or later operating systems.

For information about configuring your browsers, refer to the *Catalyst 1900 Series Installation and Configuration Guide* and the *Catalyst 2820 Series Installation and Configuration Guide*.

Features

The Catalyst 1900 and 2820 switches running firmware version 9.00.00 and above have these features:

- Cluster membership capability—The Catalyst 1900 and Catalyst 2820 switches can be added to switch clusters and managed by a Catalyst 2900 XL or a Catalyst 3500 XL command switch by meeting these requirements:
  - The Catalyst 2900 XL or Catalyst 3500 XL command switch must be running IOS software Release 12.0(5)XP or later and must have an IP address assigned.
  - The Catalyst 1900 or Catalyst 2820 switch must be running firmware version 9.x or later.
  - The Catalyst 1900 or Catalyst 2820 switch must be Cisco Discovery Protocol (CDP) version 2-enabled.
  - The Catalyst 1900 or Catalyst 2820 switch must be connected to a cluster member or to a command switch port that belongs to the management VLAN on the command switch.
- Encrypted (secret) passwords—You can assign encrypted privileged- and user-level passwords to the switch. An encrypted password can have 1 to 25 characters, including spaces and punctuation. Encrypted passwords are case sensitive.
- Secured access to management interfaces—At initial setup, you can assign a switch IP address and an unencrypted privileged-level password to the switch. You must assign a privileged password, encrypted or unencrypted, to the switch to access the Catalyst 1900 or Catalyst 2820 switch manager and to Telnet to the switch.
- Security enhancement to password recovery—On previous releases of the firmware, you could view the password from the diagnostic console, which posed a security threat to networks that used the same password for other devices in the network. When using the diagnostic console, you can now clear the switch password only if you have lost or forgotten it.
- Additional SNMP community strings—You can assign up to four read and four write community strings from the Catalyst 1900 or Catalyst 2820 switch manager.
- Clear addresses on link down—You can enable a secured switch port to remove its address associations when the port loses its link.
- TFTP Put option disabled by default—To prevent unauthorized upgrades, the Accept Upgrade Transfer from Other Hosts option default setting is disabled.
- Increased RMON history tables—The switch supports a maximum of 540 RMON history tables. However, previous releases of the firmware only supported up to 20 RMON history tables for each switch port. You can now allocate the 540 history tables among all switch ports, in any combination. For example, you can allocate 540 history tables to one switch port, or you can allocate 20 history tables among 27 ports.
- Cisco Group Management Protocol (CGMP) Fast Leave—This option enables the switch port to leave an IP multicast group immediately when all the members have left the multicast group.
- Message-of-the-day banner—From the CLI, you can create a 400-character (or 20-line) message, which appears before the management console login screen appears.

Limitations

These sections provide usage limitations for the switches.

Limitation Specific to the Catalyst 2820 Switches

After removing or inserting a module, click **Reload** to display a fresh switch image on the Home page.

Limitations for the Catalyst 1900 and Catalyst 2820 Switches

- Clicking **Reload** from any switch manager page displays a fresh copy of the Home page, not the currently displayed page.
- The switch manager does not check parameter values that are outside the value range. If you enter an invalid parameter value, the switch manager redisplays the switch manager page with the original value. Parameter value ranges are provided in the management console, the switch manager online help, and the *Catalyst 1900 Series Installation and Configuration Guide* and the *Catalyst 2820 Series Installation and Configuration Guide*.
- RMON statistics gathering has these maximum limits:
  - 27 rows in these tables: etherStatsTable, historyControlTable, alarmTable, and eventTable.
  - If you are logging events, you can have ten entries per event, and the list is circular.

Usage Guidelines

These sections provide usage guidelines for the switches:

- "Usage Guidelines Specific to the Catalyst 1900 Switches" section on page 4
- "Usage Guidelines Specific to the Catalyst 2820 Switches" section on page 5
- "Usage Guidelines for the Catalyst 1900 and Catalyst 2820 Switches" section on page 5

Usage Guidelines Specific to the Catalyst 1900 Switches

This section describes usage guidelines specific to the Catalyst 1900 switches.

- Some switches are shipped with screws installed in the top rack-mounting holes closest to the front panel. If you want to rack-mount the switch with the front panel forward, remove these screws before attaching the mounting brackets. Do not use these screws to attach the mounting brackets to the switch. Use the screws supplied with the brackets. For information on attaching the mounting brackets to the switch, refer to the *Catalyst 1900 Series Installation and Configuration Guide*.
- If you connect to the switch attachment unit interface (AUI) port, you might notice that the fan in the switch slows down. This does not affect the operation of the switch.
- If there is no link after you connect an MT-RJ fiber-optic port on a WS-C1924F-A or a WS-C1924F-EN switch to an SC port on a 100BASE-FX-compatible device, the polarity of the SC connectors on the MT-RJ patch cable and the SC port on the device might not match. Remove the SC connectors from the snap-on holder on the cable, and transpose the connectors for A and B.

- If you connect an autonegotiating 100BASE-TX port of a Catalyst 1900 switch to a device that does not autonegotiate, there could be problems establishing a link. To work around this problem, configure the switch port to either half or full duplex to match the configuration of the other device.

Usage Guidelines Specific to the Catalyst 2820 Switches

This section describes usage guidelines specific to the Catalyst 2820 switches.

- If your attempt to upgrade the ATM module firmware fails while the module is operating normally, the expansion slot LED on the switch turns amber. The module continues operation, but the module image in Flash memory is corrupted. When you reset the ATM module, it will not find a valid Cisco IOS image, and the ATM module will not pass the power-on self-test (POST). To correct this problem, repeat the firmware upgrade procedure to download a new firmware image on the ATM module.
- If you connect an autonegotiating 100BASE-TX switch module port of a Catalyst 2820 switch to a device that does not autonegotiate, there could be problems establishing a link. To work around this problem, configure the module port for either half or full duplex to match the configuration of the other device.

Usage Guidelines for the Catalyst 1900 and Catalyst 2820 Switches

This section describes usage guidelines that apply to both the Catalyst 1900 and Catalyst 2820 switches.

- The RJ-45-to-DB-9 female DTE (labeled PC) adapter is now the only adapter that ships with the Catalyst 1900 and Catalyst 2820 switches. You can order a kit (part number ACS-DSBUASYN=) containing the RJ-45-to-DB-25 female DTE adapter and RJ-45-to-DB-25 male DCE adapters from Cisco.
- The DOS diskette containing the switch firmware and device-specific MIBs is no longer shipped with the switch. You can download the latest switch firmware and MIBs from the Service and Support site on Cisco.com. For information about Cisco.com, see the "Cisco.com" section on page 15.
- Be sure that JavaScript is enabled. From Netscape Communicator 4.xx, select **Edit > Preferences > Advanced > Enable JavaScript**. JavaScript is enabled by default on Microsoft Internet Explorer.
- Be sure that the switch manager page is updated whenever you visit the page. Set the caching of pages to **Every time** on Netscape Communicator or **Once per session** on Microsoft Internet Explorer.
- You can bookmark the switch IP address to easily retrieve the switch manager for later use.
  - If you are using Netscape Communicator, choose the **Communicator** menu option, and select **Bookmarks > Add Bookmark**.
  - If you are using Microsoft Internet Explorer, choose the **Favorites** menu option, and select **Add to Favorites**.

  Do not use the right mouse-button to bookmark the switch IP address; doing so only saves the specific frame (image) of the switch manager page.

- If the switch is directly connected to a terminal or terminal emulator rather than to a modem connection, you must configure the switch to the same baud rate and character format as the terminal or emulator.

  If the switch is dialing out, the configured baud rate of the switch does not change. The Match Remote Baud rate option (auto baud) applies only when the switch is answering an incoming call and matches a rate less than or equal to the configured rate. When the call is over, the switch reverts to the last configured baud rate.
- Be sure that the port monitoring feature (used for diagnostics) is disabled during normal operation. Enabling the port monitoring feature can degrade the performance of the switch.
- Bridge group configuration is supported on the management console and the CLI, but not on the switch manager.
- When you have bridge groups enabled, the switch manager displays information only for bridge group 1.
- Do not connect a port that belongs to more than one bridge group to another port in any of those bridge groups; this causes a network loop.
- VLAN configuration is supported on the management console and the CLI, but not on the switch manager.
- Fast EtherChannel configuration is supported on the switch manager and the CLI, but not on the management console.
- When you have VLANs enabled, the switch manager displays information only for VLAN 1.
- The switch resets when you change from using VLANs to bridge groups and vice versa, and any configured options revert to the default settings. You will need to reconfigure the options that you need for VLANs or bridge groups.

  Use the System Configuration menu, CLI, or SNMP to change from VLANs to bridge groups and vice versa.
- When the switch initializes after a reset or when a port is assigned a different VLAN membership, the port experiences the complete STP transition, as specified by IEEE 802.1D, even if the Port Fast mode is enabled. When the transition is complete, the Port Fast mode setting is enforced. This process ensures that no temporary loop is formed after a reset and allows STP to safely discover the topology of the network.
- If the trunking mode is enabled after the switch initializes, the switch can take up to 5 minutes to automatically learn VTP information from the network.
- To prevent the formation of undetected loops, nontrunk ports assigned to different VLANs must not be connected to each other. Use routers to connect devices residing on different VLANs.
- When the trunking capability is enabled on a high-speed port and the default configuration is used, the port configuration on these features is ignored:
  - VLAN membership configuration for that port.
  - STP Port Fast mode (default: disabled on high-speed ports).
  - Flooding of unknown unicast and unregistered multicast packets (default: enabled).
  - Network port configuration (default: no network port is configured). When trunking is disabled, the port configurations function as configured.
- Switch configuration changes take effect immediately. However, the switch requires 30 seconds to write changed parameters to permanent storage. If you turn off the switch too soon, the changes to the switch configuration are lost the next time the system is restarted.

- While performing a firmware upgrade, the switch might not respond to commands for as long as 1 minute. This is normal and correct. If you interrupt the transfer by turning the switch off and on, the firmware could be corrupted. If this happens, follow the procedure in "Using the Diagnostic Console" in the "Troubleshooting" chapter of the *Catalyst 1900 Series Installation and Configuration Guide* or the *Catalyst 2820 Series Installation and Configuration Guide*.

Caveats

These sections describe open and resolved caveats in firmware versions 9.00.00 through 9.00.06.

Open Caveats

This section describes possible unexpected activity in firmware versions 9.00.00 through 9.00.06.

- CSCdj85607

  When using Netscape Communicator 4.xx on PCs and Sun workstations, minimized, maximized and resized pages of the Catalyst 1900 and Catalyst 2820 Switch Manager might not refresh properly.

  The workaround is to click **Reload** to refresh the page.

- CSCdj95153

  When using Netscape Communicator 4.xx on Windows 95, clicking **Apply** after making changes to the Port Security Table page sometimes displays a blank page.

  The workaround is to click **Stop** to redisplay the Port Security Table page with your saved changes.

- CSCdp16523

  The Catalyst 1900 and Catalyst 2820 switches do not support the hidden-enable password. If the switch inherits the command-switch hidden-enable password, the switch stores the password as an unencrypted password.

  The workaround is to assign a secret enable password to the command switch when your cluster contains Catalyst 1900 and Catalyst 2820 member switches.

- CSCdj87375

  Do not use these settings for the console port when upgrading the switch through the XMODEM protocol: 9600 baud, 7 data bits, 2 stop bits, and even parity.

  The workaround is to use other settings or the console port default settings (9600 baud, 8 data bits, 1 stop bit, and no parity).

- CSCdk01665

  If you use bridge groups and Spanning Tree Protocol (STP) is disabled on a bridge group, the switch does not forward the bridge protocol data units (BPDUs) received on any ports in the bridge group to other members of the bridge group. If you are running STP on the rest of your network, network loops might result if the switch connects to other switches.

  The workaround is to disable STP on *all* bridge groups so that the switch forwards received BPDUs if you want to use bridge groups with STP disabled. Assign at least one port to all bridge groups, and then disable STP for each bridge group, using the Bridge Group Spanning Tree Configuration menu (or CLI or SNMP). You can then reassign the ports to whichever group you wish.

- CSCdk66781

  Networks that use IBM Type 1 cabling with ports configured as monitor ports can have problems if the cable becomes disconnected.

  The workaround is to configure ports for half-duplex operation because the switch does not detect a loopback if the hermaphroditic connector on the cable is disconnected.

- CSCdk57978

  In a full-duplex configuration with STP disabled, the switch does not detect a loop if an IBM Type 1 cable is disconnected.

  The workaround is to configure ports for half-duplex operation if you must have STP disabled.

- CSCdk67260

  If a 100-Mbps switch port has a disconnected IBM Type 1 cable, a change to the Port Fast mode does not take effect.

  The workaround is to reset the switch.

- CSCdk67219

  If a full-duplex port is assigned to more than one bridge group and an IBM Type 1 cable is disconnected, the switch might not detect a loopback.

  There is no workaround.

- CSCdk67682

  If a nonroot switch is bridged to a root switch through full-duplex ports using IBM Type 1 cabling, the root port on the nonroot switch might take longer to reach the STP blocking state if the cabling is disconnected and creates a loopback.

  There is no workaround.

- CSCdk67157

  If a dynamic port that is assigned to a VLAN is disconnected and reconnected to a different station, the VLAN of the port is not rediscovered.

  The workaround is to change the port to half duplex so that the switch assigns the port to a new VLAN.

- CSCdk69024

  If there are two or more Catalyst 1900 or Catalyst 2820 switches connected to a Catalyst 5000 switch by using Fast EtherChannel—and if there are two stations communicating through the Catalyst 5000 switch—the switches learn the addresses of both stations from the broadcast packets sent from those stations. Flooding of unknown unicast packets can occur if one of the stations becomes disconnected from the Catalyst 5000 switch and the other station continues to send packets to that station. The flooding stops when the switches reach the specified aging time for retaining the address of the disconnected station.

  The workaround is to use the **port-channel preserve-order** command to preserve the frame transmission order on the switch port.

- CSCdj89498

  When using the Fast EtherChannel feature with VLAN trunking between two Catalyst 1900 or Catalyst 2820 switches, changing the active link might cause flooding. You can change an active link either by changing the Port Aggregation Protocol (PAgP) port priority or by disconnecting one of the high-speed links and reconnecting it.

  The workaround is to disconnect both ports to change the active link.

- CSCdk01961

  If you use VTP pruning with Fast EtherChannel, losing one connection on one high-speed link prevents pruning from working properly. This does not cause connectivity problems, but flood traffic is sent to the neighboring switch (which should drop such traffic, resulting in minimal degradation to network performance). Pruning still works in the neighboring switches.

  The workaround is to disconnect the remaining link and then to reconnect both links to restore proper operation of VTP pruning.

- CSCdp08683

  When a Catalyst 1900 or Catalyst 2820 switch is operating at the edge of a VTP domain and is subsequently configured for VTP transparent mode, trunk ports will not be in the correct pruning state.

  The workaround is to reestablish the trunk after changing the VTP mode to transparent in one of these ways:

  - Remove, and then reconnect the trunk cable to the switch.
  - Disable, and then re-enable the trunk either by using the **trunk off** and **trunk on** commands or by using the Port Configuration Menu [S] Status of Trunk option.
  - Reset the switch.

- CSCdk03911

  After you select Auto-negotiate as the 100BASE-TX port duplex mode from the Catalyst 1900 Port Management page and click **Apply**, *Auto-negotiate* appears in the Actual field while the switch and the other device negotiate the duplex mode.

  The workaround is to click the **Port** option on the switch manager menu bar to display the final duplex state of the port.

- CSCdj92758

  If you try to upgrade the module firmware from the Catalyst 2820 Switch Manager and the **Module (Slot A or B) TFTP Upgrade** button is not on the Console and Upgrade Configuration page, the module firmware is corrupted.

  The workaround is to stop the upgrade attempt from the switch manager. Use the management console to upgrade the module firmware.

- CSCdm69165

  When the switch does not have its own IP address and is a cluster member, the Telnet link on the Catalyst 1900 or Catalyst 2820 Switch Manager Home page is disabled.

  The workaround is to use the **rcommand** ***member-number*** command from the command-switch CLI to Telnet to the switch.

- CSCdj55509

  When a switch port is assigned to be the network port, unknown unicast address packets are only sent to that port. If an attached device, such as a server, is idle for longer than the specified address aging time value, the switch removes the device address from its address table. Therefore, if a network port is assigned, the switch does not forward any unknown unicast address packets destined to that device.

  The workarounds are to

  - Configure a static address for the server.
  - Increase the address aging time to a value higher than the maximum idle time for the server.

  - Enable port security on the switch port connected to the server, set the upper limit of the number of addresses the secure port can have, and set the Action Upon Address Violation option to Ignore.
  - Do not use the network port.

- CSCdj34652

  You cannot use IP to manage the switch if the management VLAN is pruned.

  The workaround is to be sure that the management VLAN is not pruned if VTP pruning is enabled.

- CSCdj92968

  When the Fast EtherChannel feature is enabled, the spanning-tree state for the port channel is shown as N/A on the Port Configuration menu for port A or port B. (The VTP pruning statistics on the VTP Statistics Report apply to the port channel as a whole, not specifically to port A or port B.)

  The workaround is to use the Fast EtherChannel Management page, the CLI, or the SNMP Bridge MIB to find out the actual state of the port channel.

Resolved Caveats in Version 9.00.06

These problems were resolved in version 9.00.06:

- CSCdx79977

  Catalyst 1900 and Catalyst 2820 switches now continue to communicate with devices that are moved from one port to another port on the switch.

- CSCdw41694

  A Catalyst 1900 switch running software version 9.00.06 no longer has severe performance degradation caused by ports without links forwarding broadcast traffic.

- CSCdw72924

  A Catalyst 1900 switch running software version 9.00.06 no longer causes address flap on uplink ports.

- CSCdx10972

  A Catalyst 1900 switch now correctly acquires a Dynamic Host Configuration Protocol (DHCP) assigned IP address after a reset.

- CSCdx06779

  When using the Cisco Secure User Registration Tool, you can now use ports one through nine on an access-layer Catalyst 1900 or Catalyst 2820 switch. The login user is assigned to a login VLAN and to a user VLAN.

- CSCdw18996

  Catalyst 1900 and Catalyst 2820 cluster member switches with a defined IP address and network gateway now continue to exchange Cluster Membership Protocol (CMP) messages with the cluster commander.

Resolved Caveats in Previous Versions

These problems were resolved in version 9.00.05:

- CSCds09069

  Catalyst 1900 and 2820 switches can now communicate with other management VLANs even if the switch has no ARP entry in its ARP table for a default gateway or does not have a port assigned to a management VLAN.

- CSCds60075

  The MIB object **IfLastChange** now reports the correct time when the LinkUp/LinkDown Traps are disabled on the switch.

- CSCdt65828

  The FDDI DAS module no longer incorrectly appears as an SAS module in a Catalyst 2820 switch.

- CSCdr56930

  The **show cdp neighbor detail** command now works correctly on the switch and no longer shows only the IP address of the command switch.

- CSCds57774

  The switch no longer fails when the HTTP server is enabled and a browser tries to access the URL http://switch-ipaddr/anytext?/.

- CSCds77252

  Catalyst 1900 and 2820 switches running Enterprise software release 9.00.05 can now answer queries for the MIB object **ipAdEntNetMask** when you use the **snmpget** command.

- CSCdt33416

  SNMP operations with null community strings are no longer allowed.

- CSCdv09114

  If a switch is installed before the DHCP scope is configured on the DHCP server, or before the DHCP server is online the switch now completes automatic configuration through TFTP.

- CSCdv11505

  Catalyst 1900 and 2820 switches now respond to ARP requests in a redundant uplink configuration where there are no access ports assigned to the management VLAN.

- CSCdv35159

  Catalyst 1900 and 2820 switches no longer allow community strings ending with a numeral or an @ symbol.

- CSCdu56824

  Catalyst 1900 and 2820 switches no longer allow privileged EXEC access with a user EXEC password.

This problem was resolved in version 9.00.04:

- CSCds28410

  Version 9.00.04 corrected a condition on the Catalyst 1900 and 2820 switches running Enterprise Edition firmware that caused VLAN Trunk Protocol (VTP) configuration information to be lost. The VTP mode changes from transparent or server mode to client mode after VTP parameters are configured. In version 9.00.03, these parameters were lost after the switch was reset, and the switch would revert back to server mode.

Note Upgrading to version 9.00.04 can cause the loss of restricted static addresses. If you have a restricted static addresses configured, save your configuration file to a TFTP server before upgrading. Upgrade to version 9.00.04, and then reload your configuration file.

This problem was resolved in version 9.00.03:

- CSCdr50274

  Version 9.00.03 corrected an anomolous user-invoked system reset condition. If you reset the system through the console interface (as opposed to recycling power), it was statistically possible for a single, random port on the unit to fail to acquire link and operate properly. You would then observe a nonfunctional or dead port. Power cycling the switch corrected the problem. The software modification reset all ports in the switch so that a port cannot lock up immediately after a user-invoked reset.

This problem was resolved in version 9.00.02:

- CSCdp70664

  Catalyst 1900 and 2820 switches no longer cause spanning-tree loops when UplinkFast is enabled.

These problems were resolved in version 9.00.01:

- CSCdp09675

  If you issue a Get_Next_Request in an SNMP MIB list on an interface, there is no longer an extra entry at the end that does not belong.

- CSCdm14589

  In a Telnet session, the paste function in the CLI configuration mode now works correctly.

These problems were resolved in version 9.00.00:

- CSCdp22047

  The CDP checksum algorithm is now compatible with the Cisco IOS software. Previously, when a CDP packet had an odd number of bytes and the value of the last byte was greater than 0x80, the device sending the packet was not recognized as a neighbor.

- CSCdm80245

  You can use a DEC Alpha 1000a BOOTP server to automatically assign an IP address to the switch.

- CSCdm85421

  The switch can now autoconfigure from a DHCP server that is *not* Windows NT.

- CSCdm87247

  You can use the ipNetToMediaEntry MIB object from a Catalyst 1900 WS-C1912 model.

- CSCdm58378

  Whether in VTP transparent or server mode, the switch drops VTP packets from blocked ports and no longer receives and sends these packets to unblocked ports.

- CSCdm83795

  The switch can use a CiscoSecure NT TACACS server to authenticate access based on the switch IP address.

Related Documentation

Use these Catalyst 1900 and Catalyst 2820 publications for firmware version 9.x with this document:

- *Catalyst 1900 Series Installation and Configuration Guide*
- *Catalyst 2820 Series Installation and Configuration Guide*
- *Installing the Cisco Catalyst 1900/2820 Enterprise Edition Software*
- *Catalyst 1900 Series and Catalyst 2820 Series Enterprise Edition Software Configuration Guide*
- *Catalyst 1900 Series and Catalyst 2820 Series Command Reference* (online only)
- *Catalyst 2820 ATM Modules Installation and Configuration Guide*
- *Catalyst 2820 Modules User Guide*

Obtaining Documentation

The following sections explain how to obtain documentation from Cisco Systems.

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at the following URL:

http://www.cisco.com

Translated documentation is available at the following URL:

http://www.cisco.com/public/countries_languages.shtml

Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which is shipped with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual subscription.

Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco Direct Customers can order Cisco product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/cgi-bin/order/order_root.pl

- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:

  http://www.cisco.com/go/subscription

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

If you are reading Cisco product documentation on the World Wide Web, you can send us your comments by completing the online survey. When you display the document listing for this platform, click **Give Us Your Feedback**.

You can e-mail your comments to bug-doc@cisco.com.

To submit your comments by mail, use the response card behind the front cover of your document, or write to the following address:

Cisco Systems, Inc.
Attn: Document Resource Connection
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools by using the Cisco Technical Assistance Center (TAC) Web Site. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC Web Site.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com is a highly integrated Internet application and a powerful, easy-to-use tool that provides a broad range of features and services to help you to

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages
- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

You can self-register on Cisco.com to obtain customized information and service. To access Cisco.com, go to the following URL:

http://www.cisco.com

Technical Assistance Center

The Cisco TAC is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two types of support are available through the Cisco TAC: the Cisco TAC Web Site and the Cisco TAC Escalation Center.

Inquiries to Cisco TAC are categorized according to the urgency of the issue:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration.
- Priority level 3 (P3)—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- Priority level 2 (P2)—Your production network is severely degraded, affecting significant aspects of business operations. No workaround is available.
- Priority level 1 (P1)—Your production network is down, and a critical impact to business operations will occur if service is not restored quickly. No workaround is available.

Which Cisco TAC resource you choose is based on the priority of the problem and the conditions of service contracts, when applicable.

Cisco TAC Web Site

The Cisco TAC Web Site allows you to resolve P3 and P4 issues yourself, saving both cost and time. The site provides around-the-clock access to online tools, knowledge bases, and software. To access the Cisco TAC Web Site, go to the following URL:

http://www.cisco.com/tac

All customers, partners, and resellers who have a valid Cisco services contract have complete access to the technical support resources on the Cisco TAC Web Site. The Cisco TAC Web Site requires a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to the following URL to register:

http://www.cisco.com/register/

If you cannot resolve your technical issues by using the Cisco TAC Web Site, and you are a Cisco.com registered user, you can open a case online by using the TAC Case Open tool at the following URL:

http://www.cisco.com/tac/caseopen

If you have Internet access, it is recommended that you open P3 and P4 cases through the Cisco TAC Web Site.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses issues that are classified as priority level 1 or priority level 2; these classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer will automatically open a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to the following URL:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

Before calling, please check with your network operations center to determine the level of Cisco support services to which your company is entitled; for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). In addition, please have available your service agreement number and your product serial number.

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.